National Infrastructure Protection Center
CyberNotes

Issue #2-99 *January 20, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at www.fbi/nipc/index.htm.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between January 1 and January 15, 1999. The table provides the operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site. Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
ACC's Tigris Access Terminal[1]	HARDWARE	Unauthorized individuals can gain access to sensitive data without logging in.	No workarounds or patches known at time of publishing.	Tigris Access Terminal Display	Medium	No scripts identified at time of publishing. Explanation of exploit available in newsgroups.
ACC's Tigris Access Terminal Operating System[2] Up to 10.5.8	Operating System	Unauthorized individuals can use the box as a telnet hopping point. The terminal also contains an apparently undocumented default account of public.	Workaround is to restrict telnet access to specific host and to disable source routing.	Tigris default password	Medium/ High	No scripts identified at time of publishing. Explanation of exploit available in newsgroups.
Fore PowerHUB[3]	HARDWARE	Nmap scan will cause the hub to halt for approximately 80 seconds.	Fore has a fix in the form of Powerhub Software 5.0.1. Non-accelerated hardware has a new software release (2.6.4.3) that	Nmap scan	Medium	Exploit script (nmap) posted to newsgroups and Web sites.

[1] BUGTRAQ, January 4, 1999.
[2] BUGTRAQ, January 4, 1999.
[3] BUGTRAQ, January 5, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
			corrects this.			Hackers known to be using.
FreeBSD[4] 2.2.5-r	Operating system (syslog)	Default configuration of FreeBSD is to allow 10 log-in attempts before a log entry is entered. Times of 30, 120 and 600 seconds are also used to log entries. Unusual system failure during this window may result in log loss.	The number of log-in attempts allowed before logging can be modified. The source is located in /usr/src/usr.bin/login/login.c.	FreeBSD syslog timing	Low	This default condition has been discussed in newsgroups.
Linux[5] (old bug that has resurfaced)	Tripwire 1.2 or earlier (part of RedHat's Linux powertools CD-ROM)	Tripwire will stop functioning and cause a core dump if it receives a filename of 128-255 characters.	An earlier published patch contained an error. Commercial version of tripwire has problem corrected. Support possible from http://www.tripwiresecurity.com	Tripwire long filename crash	Low	No scripts identified at time of publishing. Explanation of exploit available in newsgroups.
Linux - Red Hat[6] 4.2 and 5.X	Operating System (Dosemu + S-Lang)	Local user can execute a buffer overflow and gain root access.	Red Hat posted a patch in June 1998. This patch does not appear to be incorporated in the Dosemu routine of the recently released Version 5.2.	Dosemu + S-Lang	Low	Exploit scripts posted to newsgroups and Web sites.
Microsoft[7]	Excel	When using the call function in Excel some executables can be run without the user's knowledge.	Patch is available at: http://offficeupdate.microsoft.com/downloaddetails/x197cfp.htm	Excel call function vulnerability (a.k.a. Russian New Year exploitation)	Medium/ High (Risk increase from the Jan 6 CyberNotes due to publicity)	Attack scripts have been discussed on hacker IRC channels.
Microsoft Windows[8] 95, 98, and NT	Internet Explorer (IE) 4.0, 4.1, and 5 beta	Latest Java Virtual Machine (JVM) has reintroduced a hostile applet attack. These applets will cause 95 and 98 to crash. On NT machines, IE will crash.	Patches are available at: http://www.microsoft.com/java/vm/dl_vm31.htm or http://www.microsoft.com/windows/ie/download/jvm.htm.	Java hostile applet	Medium/ High	Exploit scripts posted to newsgroups and Web sites. Attacks have occurred in the past.

[4] BUGTRAQ, January 2, 1999.
[5] BUGTRAQ, January 4, 1999.
[6] BUGTRAQ, January 4, 1999.
[7] Microsoft Security Bulletin (MS98-018).
[8] Newsbytes, January 4, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows[9] 95, 98, and NT	Operating System	Between April 1, 2001, and April 8, 2001, Microsoft Windows applications will believe that it is one hour earlier.	Microsoft has stated that a release date for the fix is not available at this time.	April fool's 2001 bug	Low (unless you have time critical functions)	Bug has been discussed on various newgroups.
Microsoft Windows 98[10]	Novell Intranetware Client	Nmap scan on port 427 will cause a critical error to develop (Blue Screen) and network connectivity to be lost.	No workarounds or patches known at time of publishing.	Nmap Scanning	Medium/ High	Exploit script (nmap) posted to newsgroups and Web sites. Hackers known to be using nmap with increased frequency.
Microsoft Windows 98[11] (CORRECTION[12])	Operating System	Nmap scan will cause a critical error to develop (Blue Screen) and network connectivity to be lost.	Organization that published this advisory has updated it. The new advisory states that default installation of Windows 98 is not vulnerable (see new listing Microsoft Windows 98. - Novell Intranetware Client).	Nmap scanning	Medium/ High	Exploit script (nmap) posted to newsgroups and Web sites. Hackers known to be using.
Microsoft Windows[13] 9X	Operating System (system acting as file servers)	It is possible to sniff the Challenge Response sequence and replay it for 15 minutes. This allows an unauthorized user to assume the identity of an authorized user.	Suggested workaround disables LM Authentication, resulting in the inability to use 9X boxes as file servers.	Window 9X Challenge Response Timeout	Medium/ High	Bug has been discussed on various newgroups. Hackers typically install sniffers on networks. Sniffers will capture the Challenge Response sequence.
Sun Solaris[14] 2.5, 2.5.1, 2.6, and, 2.7 (Note: advisories have been previously issued regarding this vulnerability)	Operating System (Automount and rpc.statd)	Unauthorized user can gain root by sending specific remote procedure call (rpc) packets.	Patch is available that partially corrects this problem. Patch is available from: http://sunsolve.com/sunsolve/pubpatches/patches.html	Solaris Automount	High	Exploit script posted to newsgroups and Web sites. Hackers known to be exploiting.
Sun Solaris[15] 2.7 (See Note at end of table)	Operating System (ufsdump)	Buffer overflow conditions exists in ufsdump that can allow an unauthorized user to gain root access.	Patch is available from: http://sunsolve.com/sunsolve/pubpatches/patches.html	Solaris ufsdump	High	Exploit script posted to newsgroups and Web sites. Hackers known to be exploiting this overflow.
Sun Solaris[16] 2.5.1 and 2.6	Operating System	Unauthorized user can rename files. This can result in manipulation of the file system to provide a root log-in.	Workaround is to chmod ug-s /usr/openwin/bin/ff.core. Note that this exploit is very dependent on system configuration.	Sun Solaris ff.core	Medium	Exploit script posted to newsgroups and Web sites.

[9] NTBUGTRAQ, January 7, 1999.
[10] SecureXpert labs Advisory SX-98.12.30-01.
[11] SecureXpert labs Advisory SC-98.12.23-01.
[12] SecureXpert labs Advisory SX-98.12.30-01.
[13] L0pht Security Advisory, January 5, 1999.
[14] BUGTRAQ, January 3, 1999.
[15] BUGTRAQ, January 2, 1999.
[16] BUGTRAQ, January 7, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix[17]	L0phtcrack 2.5	Creates temporary files in the system TEMP directory. These files contain password hashes. If auto-save is used, cracked passwords will be stored in the TEMP directory.	New version has been made available at: http://www.l0pht.com/l0phtcrack/dist/l0phtcrack251.exe	L0phtcrack temporary files	Medium/ High	No scripts identified at time of publishing. Explanation of exploit available in newsgroups.
Unix[18]	suGuard	Any user can gain root access to the system.	No workarounds or patches known at time of publishing.	SuGuard pathing problem	High	Exploit scripts posted to newsgroups and Web sites.
Unix and Microsoft Windows[19]	mSQL	Multiple buffer overflows exist in the program that may allow unauthorized users to execute commands.	No workarounds or patches known at time of publishing.	MSQL buffer overflows	High	Exploit scripts posted to newsgroups and Web sites.

Note: If you have recently purchased a CD-ROM, it is possible that patches released several weeks before your purchase are not included on the CD-ROM. CD-ROM's generally have cut off dates for software additions weeks before they are available for purchase.

*Risk is defined in the following manner:

High – A vulnerability that will allow an intruder to immediately gain privileged access (e.g., Sysadmin, root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium – Any vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[17] NTBUGTRAQ, January 6, 1999.
[18] L0pht Security Advisory, January 3, 1999.
[19] Brazilian Information Security Team, 01/99

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between January 1 and January 15, 1999, listed by date of script, script name, script description, and testing conducted. Items listed in boldface (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches. Those items in red represent scripts that hackers/crackers are utilizing. During this time period, 50 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Testing Conducted**
Jan 14, 1999	Ath0-2.sh	Shell script to exploit “+++ATH0” DoS attack against Unix boxes running modems.	
Jan 14, 1999	**Bogtk v1.0.1**	**Linux/Unix Back Orifice client graphical user interface.**	
Jan 13, 1999	IPTraf v1.4.2	A monitor that collects Local Area Network (LAN) statistics, checksums, and packet information.	
Jan 13, 1999	Namp	Network scanning tool that has a variety of scanning modes, including stealth, Xmas, and Null stealth. Note: This tool is being used by hackers and may cause systems to become unstable.	
Jan 12, 1999	Proxys-4-all	Explanation of how to use proxies for anonymous Web surfing. Includes a list of sites that allow anonymous Web surfing.	
Jan 11, 1999	Domscan 2.0pl	A domain scanner written in Perl.	
Jan 11, 1999	Gammaprog 1.4	Bruteforce password cracker for Web-based and Point-of-Presence 3 (POP3) e-mail addresses.	
Jan 11, 1999	**GetadmforSop**	**Exploit that elevates privileges to both local and global Administrator level.**	
Jan 11, 1999	**K2v1017**	**Program that allows remote user access to current and old dial-up networking passwords, also shows passwords hidden behind asterisks (*).**	
Jan 11, 1999	MSQL-DoS.txt	Explanation of several buffer overflows that exist in MSQL.	
Jan 11, 1999	**Netboot v0.9.0b**	**Allows booting of computer with Intel processor via an Internet Protocol (IP) network.**	
Jan 11, 1999	**Pass10**	**Program that shows passwords hidden behind asterisks (*).**	
Jan 11, 1999	S10scan v0.1	Sends large volume of “fake scans” with “real scans” embedded within.	
Jan 11, 1999	SDI-msql	Exploit code for the mSQL vulnerabilities (several buffer overflows.)	
Jan 11, 1999	SilentBot	Silent bot for IRCs.	
Jan 11, 1999	Trojanit	Trojan horse/root kit for Linux. Some code included for Berkeley Software Distribution (BSD) root kit.	
Jan 10, 1999	Arptool	Program written in C that can map the IP of machines on the same Ethernet segment and can be used for spoofing hosts.	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Testing Conducted**
Jan 10, 1999	BoClient 1.4.1	Back Orifice with built-in Transmission Control Protocol (TCP) send/receive and the ability to remember most parameters.	
Jan 10, 1999	ff.core.sh	Exploit script for the ff.core vulnerability listed in "Bugs, Holes, & Patches" table above.	
Jan 10, 1999	Mother2	Shell script that finds all setuid and setgid programs.	
Jan 10, 1999	Nessus WIP 010999	Security audit tool that has 180 plug-ins for checking known holes. (Earlier version found to contain a Trojan horse.)	
Jan 10, 1999	Sucker v0.1	Shell script that checks for various vulnerabilities in a TCP/IP-based network.	
Jan 10, 1999	Tcpscan v1.02	TCP port scanner.	
Jan 7, 1999	Exploits	A 3.1megabyte (MB) file that contains 1000 exploits that have been sorted and categorized.	
Jan 7, 1999	ICMP	Program that uses Internet Control Message Protocol (ICMP) packets to obtain information from remote hosts. This program supports spoofing and broadcasting.	
Jan 7, 1999	Lanlord v0.1.1	Program designed to discover what machine has which Dynamic Host Configuration Protocol (DHCP) address.	
Jan 6, 1999	Cheops v0.59a	Tool for network scanning and discovery of operating system. Note: The author of the tool has posted warnings that the tool has the potential of being misused and there have been indications that hackers are currently using this tool.	
Jan 6, 1999	Cyberanon v1.1	Common Gateway Interface (CGI) script anonymizer that attempt to allow users to surf the web anonymously.	
Jan 6, 1999	L0phtCrack 2.51 for Win95/NT	Password cracker for Microsoft Windows 95/NT.	
Jan 6, 1999	**Net-RawIP v 0.03f**	**Perl module that manipulates raw IP packets and Ethernet headers.**	
Jan 6, 1999	Novell-iwc-DoS	DoS explanation for the Novell Intranet Client vulnerability (see "Bugs, Holes, & Patches" above.)	
Jan 6, 1999	Oracle8-tnslsnr-DoS	DoS explanation for the Oracle version 8 DoS vulnerability (see January 6, 1999, edition of CyberNotes.)	
Jan 6, 1999	Pwdump2	Program that dumps the password hashes from NT's SAM database without SYSKEY enabled.	
Jan 6, 1999	Qmail-DoS-anonymous	A number of DoS attack scripts against Qmail.	
Jan 6, 1999	Windows File Sharing hole	Explanation of the authentication timing problem with Microsoft Windows 95 (see "Bugs, Holes, & Patches" above.)	
Jan 4, 1999	Automountd exploit	Program to exploit the Automountd vulnerability in Sun Solaris (see "Bugs, Holes, & Patches" above.)	
Jan 4, 1999	Bus Conquerer v1.3	Scans for the NetBus program, cracks the password and then reassigns a new password.	
Jan 4, 1999	Either	Program for modification of MAC addresses on Microsoft Windows machines.	
Jan 4, 1999	EliteSys Entry v2.05	Brute force password cracker for File Transfer Protocol (FTP), Web, and POP3 machines.	
Jan 4, 1999	GnuSniff v0.0.5	Packet sniffer.	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Testing Conducted**
Jan 4, 1999	Mirc-hidden-files	Exploit program for ICQ “hidden file” security hole.	
Jan 4, 1999	**Net-RawIP v 0.03e**	**See entry above.**	
Jan 4, 1999	**Suguard**	**Exploit code for DataLynx’s SuGuard (see “Bugs, Holes & Patches” above.)**	
Jan 4, 1999	Termz.c	Exploit code for the S-Lang buffer overflow in Red Hat Linux (see “Bugs, Holes, & Patches” above.)	
Jan 4, 1999	Web Cracker v2.0	Brute force password cracker for Web sites.	
Jan 3, 1999	**Bogtk v1.0**	**See entry above.**	
Jan 3, 1999	Exscan v0.3	Port scanner with a strobe scanning capability.	
Jan 2, 1999	Electronic Civil Disobedience Disturbance Developer’s Kit	Explanation and code for flooding a host server with requests.	
Jan 2, 1999	Gammaprog 1.3	See description above (Gammaprog 1.4).	
Jan 1, 1999	Ufodump	Local root exploit for the ufsdump vulnerability in Solaris 2.6	

Trends

1. Several hackers/hacker groups appear to be using coordinated scans and probes from different sites.
2. More phreaker tools are appearing on hacker Web sites.
3. Increase in organized crime using compromised Private Automatic Branch Exchanges (PABXs.)
4. Scanning for Internet Map Access Protocol (IMAP) and POP continues.
5. Significant increase in reports of NetBus and BackOrifice scanning.
6. Large increase in the number of scans directed specifically against Domain Name Servers.

Viruses

During the last quarter, anti-virus vendors have reported that there has been a sharp increase (5 - time increase over the same period last year) in the number of customers submitting files suspected of containing viruses. The contaminated files during the quarter were classified in the following manner: 45 to 50 percent contained Trojan horses, 25 to 30 percent contained a macro virus, approximately 20 percent contained a file virus, and 3 to 5 percent contained multi-partite viruses.

In the last two weeks, there has been an increase in reports of many people receiving e-mail messages with Trojan horse programs attached. The most prevalent of these appears to be the picture.exe (aka. URLsnoop) Trojan horse program. Most major anti-virus vendors have included code in their latest data file updates to detect this Trojan horse program.